======= **WPI** =======

TI - Code key generator securing confidentiality in digital communication - includes operators having different algorithms in parallel to obtain n-bit output against 2n-bit input key and has random number generator against 2n-bit input key NoAbstract Dwg 1/6

AB - J04117038

PN - JP4117038 A 19920417 DW199222 H04L9/28 005pp

PR - JP19900232851 19900903

PA - (MITQ) MITSUBISHI ELECTRIC CORP

MC - W01-A05A

DC - W01

IC - H04L9/02 ;H04L9/28

AN - 1992-179912 [22]

======= **PAJ** =======

TI - CRYPTOGRAPHIC KEY GENERATOR

AB - PURPOSE:To prevent leakage of cryptography by activating plural arithmetic units with different algorithm to obtain an n-bit output with respect to an input key in 2n-bit in parallel, generating a random number on the one hand, selecting an n-bit output among outputs of the arithmetic units so as to use it as a cryptographic key.

- CONSTITUTION:A distribution circuit 13 distributes a 2n-bit input key into two sets of high-order and low-order n-bit strings and arithmetic circuits 14-a, 15-a, 14-b, 15-b convert two sets of n-bit strings in high and low orders outputted from the distribution circuit 13 into one set of n-bit string. Random number generating circuits 16-a, 16-b generate a random number with respect to the 2n-bit input key and selector circuits 17-a, 17-b select outputs of the arithmetic circuits 14-a, 15--a, 14-b, 15-b according to the random number outputted from the random number generating circuits 16-a, 16-b as a cryptographic key. Thus, the estimate and decoding of the cryptographic key by a 3rd party are made difficult and the leakage of cryptography is prevented.

PN - JP4117038 A 19920417

PD - 1992-04-17

ABD - 19920807

ABV - 016367

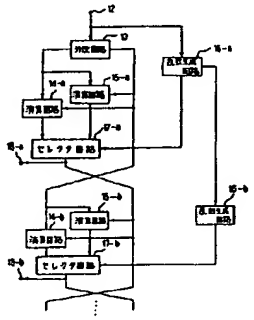
AP - JP19900232851 19900903

GR - E1245

PA - MITSUBISHI ELECTRIC CORP

IN - NAKAMURA TAKAHIKO

I - H04L9/28



<First Page Image>

This Page Blank (uspto)

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平4－117038

⑤1Int. Cl.⁵　識別記号　庁内整理番号　⑬公開　平成4年(1992)4月17日

H 04 L 9/28　7117－5K　H 04 L 9/02　A

審査請求　未請求　請求項の数 1　（全5頁）

⑤4発明の名称　暗号鍵生成装置

⑳特　願　平2－232851

㉒出　願　平2(1990)9月3日

⑦2発明者　中村　隆彦　神奈川県鎌倉市大船5丁目1番1号　三菱電機株式会社情報電子研究所内

⑦1出願人　三菱電機株式会社　東京都千代田区丸の内2丁目2番3号

⑦4代理人　弁理士　宮園　純一

明　細　書

1. 発明の名称

暗号鍵生成装置

2. 特許請求の範囲

2nビットの入力鍵に対して上位nビットと下位nビットとの2組のnビットのビット列に分配する分配回路と、この分配回路から出力された上位nビットと下位nビットとの2組のnビットのビット列に対して1組のnビットのビット列に変換する演算を行うアルゴリズムの異なる複数個の演算回路と、上記2nビットの入力鍵に対し乱数を生成する乱数生成回路と、この乱数生成回路から出力された乱数に従って上記複数個の演算回路の出力を選択し暗号鍵とするセレクタ回路とを備えたことを特徴とする暗号鍵生成装置。

3. 発明の詳細な説明

〔産業上の利用分野〕

この発明はディジタル通信において通信情報の秘密を守るための暗号鍵を生成する暗号鍵生成装置に関するものである。

〔従来の技術〕

第5図は例えば、電子情報通信学会論文誌Vol J70－D No.7(pp.1413～1423)の「高速データ暗号アルゴリズムFEAL」に示された従来の暗号鍵生成装置の構成を示すブロック図である。第5図において、1は64ビットの入力鍵が入力される入力端子、2は64ビットの入力に対し上位32ビットと下位32ビットに分配する分配回路、3－a～3－dは64ビットの入力に対し、一定のアルゴリズムに従って32ビットの出力を計算する演算回路、4－a～4－cはEXOR回路（排他的論理和回路）、5－a～5－dは演算回路3－a～3－dで計算された各暗号鍵を出力する出力端子である。また、第6図は、演算回路3－a～3－dの内部構成を示すブロック図である。第6図において、6－a，6－bは32ビットの入力が行われる入力端子、7－a，7－bは32ビットの入力に対し、8ビットずつ4つのブロックに分配する分配回路、8はEXOR回路、9は3入力に対し2^8を法として加算し、2

ビット・ローテード・シフトする加算シフト回路、10は8ビット4ブロックを32ビットシリアルに変換する選択回路、11は演算回路の出力端子である。

次に動作について説明する。まず、入力端子1から64ビットの入力鍵が入力され、分配回路2で上位32ビットと下位32ビットに分配される。分配回路2で分配された上位32ビットと下位32ビットは演算回路3－aに入力される。演算回路3－aに入力されたビットは、それぞれ分配回路7－a，7－bで8ビットごとに分配され、EXOR回路8と加算シフト回路9で演算を行い、選択回路10で32ビットシリアルにし、演算回路3－aから出力端子5－aに出力させる。以下、同様の操作を、第4図の矢印の方向に従って計算し、演算回路3－b，3－c，3－dの32ビットの出力をそれぞれ出力端子5－b，5－c，5－dに出力させ、暗号鍵とし、図示しない暗号文生成装置に入力させる。

〔発明が解決しようとする課題〕

従来の暗号鍵生成装置は以上のように構成されているので、入力鍵が当該通信関係者以外の第三者に漏れると、その入力鍵に基づいて暗号鍵が容易に推定され、暗号が容易に解読されるという問題点があった。

この発明は上記のような問題点を解決するためになされたもので、第三者による暗号鍵の推定および暗号の解読を困難にし、暗号の漏洩を防止することができる暗号鍵生成装置を得ることを目的とする。

〔課題を解決するための手段〕

この発明に係る暗号鍵生成装置は、2nビットの入力鍵に対して上位nビットと下位nビットとの2組のnビットのビット列に分配する分配回路13と、この分配回路13から出力された上位nビットと下位nビットとの2組のnビットのビット列に対して1組のnビットのビット列に変換する演算を行うアルゴリズムの異なる複数個の演算回路14－a，15－a，14－b，15－bと、上記2nビットの入力鍵に対し乱数を生成する乱数生成回路16－a，16－bと、この乱数生成回路16－a，16－bから出力された乱数に従って上記複数個の演算回路14－a，15－a，14－b，15－bの出力を選択し暗号鍵とするセレクタ回路17－a，17－bとを備えたものである。

〔作用〕

分配回路13は、2nビットの入力鍵に対して上位nビットと下位nビットとの2組のnビットのビット列に分配する。演算回路14－a，15－a，14－b，15－bは分配回路13から出力された上位nビットと下位nビットとの2組のnビットのビット列に対して1組のnビットのビット列に変換する。乱数生成回路16－a，16－bは上記2nビットの入力鍵に対し乱数を生成する。セレクタ回路17－a，17－bは乱数生成回路16－a，16－bから出力された乱数に従って演算回路14－a，15－a，14－b，15－bの出力を選択し暗号鍵とする。

〔実施例〕

第1図はこの発明の一実施例に係る暗号鍵生成装置の構成を示すブロック図である。第1図において、12は例えば64ビットの入力鍵が入力される入力端子、13は64ビットの入力鍵に対して上位32ビットと下位32ビットとの2組のnビットのビット列に分配する分配回路、14－a，14－bは分配回路13から出力された上位32ビットと下位32ビットとの2組の32ビットのビット列（64ビット）の入力に対し一定のアルゴリズムに従って1組の32ビットのビット列に変換する演算を行う演算回路、15－a，15－bは上記の演算回路14－a，14－bとは別のアルゴリズムによって、64ビットの入力鍵から32ビットのビット列に変換する演算を行う演算回路である。16－a，16－bは64ビットの入力鍵に対し例えば1ビットの乱数を生成し出力する乱数生成回路、17－aは演算回路14－aの出力と演算回路15－aの出力から、乱数生成回路16－aの出力に応じて一方を選択し、暗号鍵を出力するセレクタ回路である。17－bも

セレクタ回路17－aと同様に、演算回路14－b，15－bの出力から乱数生成回路16－bの出力である乱数に応じて、一方を選択し、暗号鍵を出力するセレクタ回路、18－a，18－bはそれぞれセレクタ回路17－a，17－bで出力される暗号鍵を出力する出力端子である。なお、この第1図に示す回路は以下同様な構成で同様な操作をくり返す。

第2図(a)は第1図中の演算回路14－a，14－bの一構成例を示すブロック図である。第2図(a)，(b)において、19－a，19－b，19－c，19－dは演算回路の入力端子、20－a，20－bはEXOR回路、21－a，21－b，21－cは入力ビットに対しローテードシフトを行うシフト演算回路、22－a，22－b，22－cは3入力に対し加算操作とローテードシフト操作を行う加算シフト回路、23－a，23－bは演算回路の出力端子である。

第3図は第1図中の乱数生成回路16－a，16－bの一構成例を示すブロック図であり、予めフラグビットを決定しておき、そのフラグビットの内容によって第1図中のセレクタ回路17－a，17－bの動作を決定する。

次にこの実施例の動作について説明する。第1図において、まず、入力端子12から64ビットの入力鍵が入力され、分配回路13で上位32ビットと下位32ビットに分配される。分配された入力鍵は演算回路14－aおよび演算回路15－aに入力される。演算回路14－aにおいては、第2図(a)に示すように入力端子19－a，19－bから分配回路13の出力である32ビットのビット列がそれぞれ入力される。入力端子19－aから入力された32ビットのビット列は、シフト演算回路21－aにおいて1ビット・ローテード・シフトされ、EXOR回路20－aにおいてシフト演算回路21－aの出力と入力端子19－bから入力された32ビットのビット列との排他的論理和がとられ、加算シフト回路22－aに入力される。

また、入力端子19－bから入力された32ビットのビット列は、一方でシフト演算回路21－bに入力されて1ビット・ローテード・シフトし、加算シフト回路22－aに入力される。加算シフト回路22－aでは2組の32ビットの入力ビット列に対して排他的論理和をとり、それに1ビット・ローテード・シフト操作を行い、2^{32}を法として1を加算した結果の32ビットのビット列を出力端子23－aから出力する。

また、演算回路15－aにおいては、第2図(b)に示すように入力端子19－c，19－dから分配回路13の出力である32ビットのビット列がそれぞれ入力される。入力端子19－c，19－dから入力された2組の32ビットのビット列は加算シフト回路22－bに入力されて排他的論理和がとられ、それに1ビット・ローテード・シフト操作が行われ、2^{32}を法として1を加算した結果がシフト演算回路21－cに入力され、1ビット・ローテード・シフトし、加算シフト回路22－cに入力される。もう一方で、入力端子19－c，19－dから入力された2組の32ビットのビット列は、EXOR回路20－bに入力されて排他的論理和がとられ、加算シフト回路22－cに入力される。

加算シフト回路22－cでは、2組の32ビットの入力ビット列に対して排他的論理和をとり、それに1ビット・ローテード・シフト操作を行い、2^{32}を法として1を加算した結果の32ビットのビット列を出力端子23－bから出力する。

一方、入力鍵は第3図に示されているように組合わせ論理回路によって変換が施され、フラグビットの値によってセレクタ回路17－aが演算回路14－a，15－aの出力のいずれをとるかを選択し、出力端子18－aから演算結果を出力する。以下、第1図に示されている矢印に従って同様の操作をくり返し行い、暗号鍵を生成する。

なお、上記実施例では演算回路を2つ並列に並べて、それらの出力のうち一方を選択して暗号鍵としていたが、セレクタ回路で選択された暗号鍵を図示しない暗号文生成装置の1段目の暗号鍵とし、セレクタ回路で選択されなかった暗号鍵を、

暗号文生成装置の2段目の暗号鍵としてもよい。すなわち、第4図に示すように、乱数生成回路の出力を反転させたものに応じて動作するセレクタを付加すると上記の回路が構成される。なお、図中23はインバータ回路であり、第1図と同一符号のものは同一機能をあらわす。

〔発明の効果〕

以上のように本発明によれば、2nビットの入力鍵に対してnビットの出力を得るためのアルゴリズムの異なる複数個の演算装置をパラレルに動作させ、一方では乱数を発生させて上記演算装置の出力のうちの1組のnビットの出力を選択し、暗号鍵とする構成としたので、複数個の暗号鍵の候補が生成され、乱数の生成方法に応じ、同じ入力鍵から異なった暗号鍵が生成でき、これにより第三者による暗号鍵の推定および暗号の解読が困難になり、したがって暗号の漏洩を防止できるという効果が得られる。

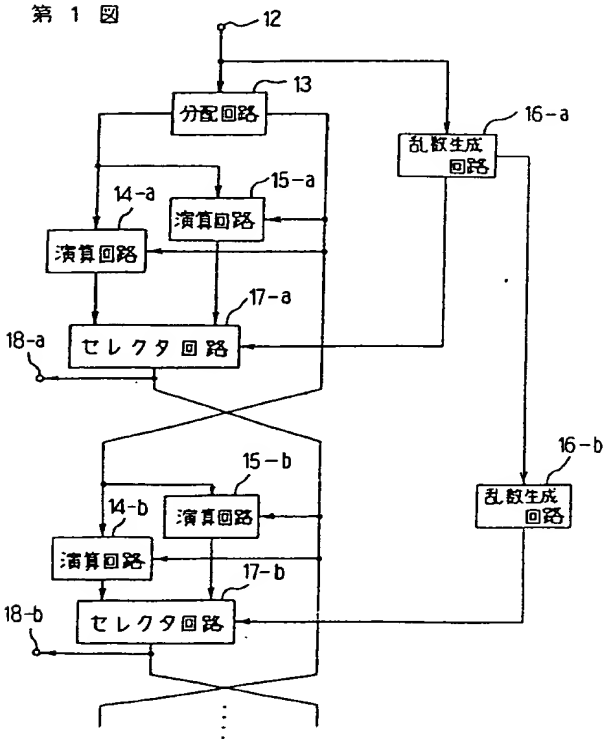
4. 図面の簡単な説明

第1図はこの発明の一実施例に係る暗号鍵生成装置の構成を示すブロック図、第2図(a)，(b)は第1図中の演算回路の一構成例を示すブロック図、第3図は第1図中の乱数生成回路の一構成例を示すブロック図、第4図は他の実施例に係る暗号鍵生成装置の構成を示すブロック図、第5図は従来の暗号鍵生成装置の構成を示すブロック図、第6図は第5図中の演算回路の内部構成を示すブロック図である。

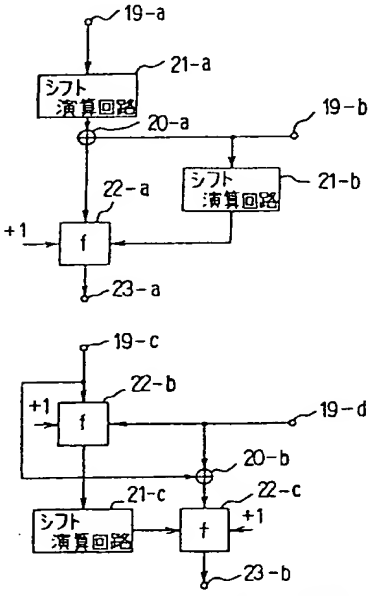
13・・・分配回路、14－a，14－b，15－a，15－b・・・演算回路、16－a，16－b・・・乱数生成回路、17－a，17－b・・・セレクタ回路。

代理人　弁理士　宮　園　純　一

第1図

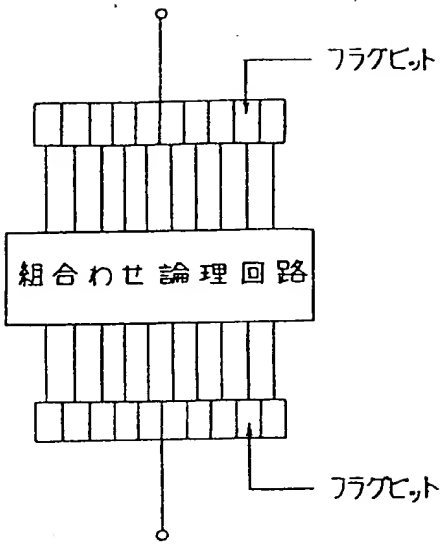


第2図

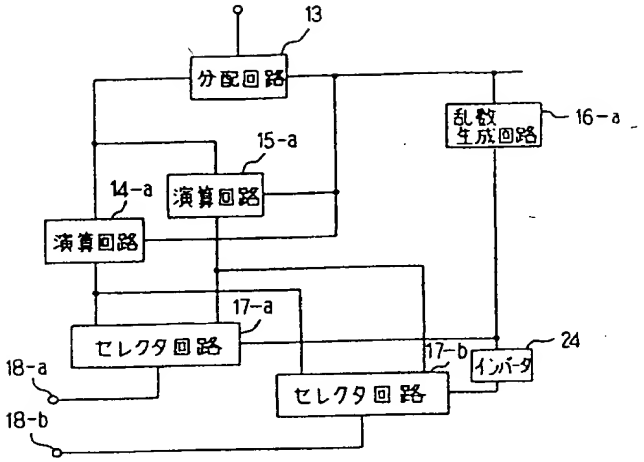


19-a，19-b，19-c，19-d；入力端子
20-a，20-b；EXOR回路
22-a，22-b，22-c；加算シフト回路
23-a，23-b；出力端子

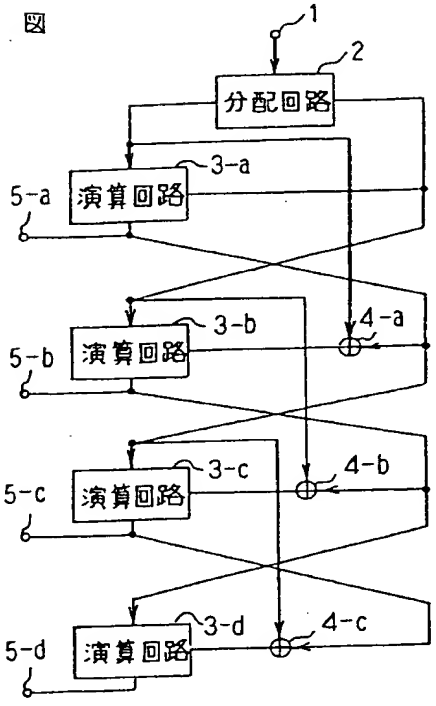
第 3 図



第 4 図



第 5 図



第 6 図